UNITED STATES PATENT AND TRADEMARK OFFICE

UNITED STATES DEPARTMENT OF COMMERCE
United States Patent and Trademark Office
Address: COMMISSIONER FOR PATENTS
P.O. Box 1450
Alexandria, Virginia 22313-1450
www.uspto.gov

APPLICATION NO.	FILING DATE	FIRST NAMED INVENTOR	ATTORNEY DOCKET NO.	CONFIRMATION NO.
09/918,831	08/01/2001	Petrus Lambertus Adrianus Roelse	NL 000444	4772

24737 7590 04/12/2006

PHILIPS INTELLECTUAL PROPERTY & STANDARDS
P.O. BOX 3001
BRIARCLIFF MANOR, NY 10510

EXAMINER	
PYZOCHA, MICHAEL J	
ART UNIT	**PAPER NUMBER**
2137	

DATE MAILED: 04/12/2006

Please find below and/or attached an Office communication concerning this application or proceeding.

Office Action Summary	Application No.	Applicant(s)	
	09/918,831	ROELSE, PETRUS LAMBERTUS ADRIANUS	
	Examiner	Art Unit	
	Michael Pyzocha	2137	

-- The MAILING DATE of this communication appears on the cover sheet with the correspondence address --

Period for Reply

A SHORTENED STATUTORY PERIOD FOR REPLY IS SET TO EXPIRE 3 MONTH(S) OR THIRTY (30) DAYS, WHICHEVER IS LONGER, FROM THE MAILING DATE OF THIS COMMUNICATION.

- Extensions of time may be available under the provisions of 37 CFR 1.136(a). In no event, however, may a reply be timely filed after SIX (6) MONTHS from the mailing date of this communication.
- If NO period for reply is specified above, the maximum statutory period will apply and will expire SIX (6) MONTHS from the mailing date of this communication.
- Failure to reply within the set or extended period for reply will, by statute, cause the application to become ABANDONED (35 U.S.C. § 133). Any reply received by the Office later than three months after the mailing date of this communication, even if timely filed, may reduce any earned patent term adjustment. See 37 CFR 1.704(b).

Status

1)☒ Responsive to communication(s) filed on *20 March 2006*.

2a)☐ This action is **FINAL**. 2b)☒ This action is non-final.

3)☐ Since this application is in condition for allowance except for formal matters, prosecution as to the merits is closed in accordance with the practice under *Ex parte Quayle*, 1935 C.D. 11, 453 O.G. 213.

Disposition of Claims

4)☒ Claim(s) *1-8 and 11-16* is/are pending in the application.

4a) Of the above claim(s) _____ is/are withdrawn from consideration.

5)☒ Claim(s) *16* is/are allowed.

6)☒ Claim(s) *1,2,6-8,11 and 15* is/are rejected.

7)☐ Claim(s) *3-5 and 12-14* is/are objected to.

8)☐ Claim(s) _____ are subject to restriction and/or election requirement.

Application Papers

9)☐ The specification is objected to by the Examiner.

10)☐ The drawing(s) filed on _____ is/are: a)☐ accepted or b)☐ objected to by the Examiner.

Applicant may not request that any objection to the drawing(s) be held in abeyance. See 37 CFR 1.85(a).

Replacement drawing sheet(s) including the correction is required if the drawing(s) is objected to. See 37 CFR 1.121(d).

11)☐ The oath or declaration is objected to by the Examiner. Note the attached Office Action or form PTO-152.

Priority under 35 U.S.C. § 119

12)☐ Acknowledgment is made of a claim for foreign priority under 35 U.S.C. § 119(a)-(d) or (f).

a)☐ All b)☐ Some * c)☐ None of:

1.☐ Certified copies of the priority documents have been received.

2.☐ Certified copies of the priority documents have been received in Application No. _____.

3.☐ Copies of the certified copies of the priority documents have been received in this National Stage application from the International Bureau (PCT Rule 17.2(a)).

* See the attached detailed Office action for a list of the certified copies not received.

Attachment(s)

1) ☒ Notice of References Cited (PTO-892)
2) ☐ Notice of Draftsperson's Patent Drawing Review (PTO-948)
3) ☐ Information Disclosure Statement(s) (PTO-1449 or PTO/SB/08) Paper No(s)/Mail Date _____.
4) ☒ Interview Summary (PTO-413) Paper No(s)/Mail Date. _____ .
5) ☐ Notice of Informal Patent Application (PTO-152)
6) ☐ Other: _____.

DETAILED ACTION

1. Claims 1-8 and 11-16 are pending.

2. Amendment filed 03/20/2005 has been received and considered.

Claim Rejections - 35 USC § 103

3. The following is a quotation of 35 U.S.C. 103(a) which forms the basis for all obviousness rejections set forth in this Office action:

> (a) A patent may not be obtained though the invention is not identically disclosed or described as set forth in section 102 of this title, if the differences between the subject matter sought to be patented and the prior art are such that the subject matter as a whole would have been obvious at the time the invention was made to a person having ordinary skill in the art to which said subject matter pertains. Patentability shall not be negatived by the manner in which the invention was made.

4. Claims 1, 7 and 8 are rejected under 35 U.S.C. 103(a) as being unpatentable over Rijmen et al (The Cipher SHARK), further in view of Loureiro et al (Function Hiding Based on Error Correcting Codes) and further in view of Knudsen et al (Hash Functions on Block Ciphers and Quaternary Codes).

As per claims 1, 7 and 8, Rijmen et al discloses a method of generating a linear transformation matrix A for use in a symmetric-key cipher, the method including: an input for receiving an input data block; creating a linear transformation matrix A with by: generating a binary (n,k,d) error-correcting

code, represented by a generator matrix $\mathbf{G} \in Z_2^{kxn}$ in a standard form $\mathbf{G} = (I_k \| B)$, with $B \in Z_2^{kx(n-k)}$, where $k < n < 2k$, and d is the minimum distance of the binary error-correcting code (see page 4), and forming a nonsingular matrix with $2k-n$ columns; and transforming the input (see page 5).

Rijmen et al fails to disclose extending matrix B, and deriving a matrix A from matrix C.

However, Loureiro et al teaches such an extension and derivation (see section 4.1).

At the time of the invention it would have been obvious to a person of ordinary skill in the art to use Loureiro et al's extending and deriving in Rijmen et al's ciphering method.

Motivation to do so would have been to hide a function represented on a matrix format.

The modified Rijmen et al and Loureiro et al method fails to disclose shortening this code.

However, Knudsen et al discloses shortening error-correcting codes (see pages 3 and 11).

At the time of the invention it would have been obvious to a person of ordinary skill in the art to use the shortening error-correcting codes method of Knudsen et al to shorten the codes of the modified Rijmen et al and Loureiro et al method.

Motivation to do so would have been that shortening codes decreases the likelihood of having a collision (see Knudsen et al pages 3 and 11).

5. Claims 2 and 11 are rejected under 35 U.S.C. 103(a) as being unpatentable over the modified Rijmen et al, Loureiro et al, and Knudsen et al method as applied to claims 1 and 8 above, and further in view of FOLDOC.

As per claims 2 and 11, the modified Rijmen et al, Loureiro et al, and Knudsen et al method discloses the step of extending matrix B with $2k-n$ columns includes randomly generating $2k-n$ columns, each with k binary elements, and forming a test matrix consisting of the $n-k$ columns of B and the $2k-n$ generating columns (see Loureiro et al section 4.1) and using the nonsingular matrix as matrix C (see Rijmen et al page 5).

The modified Rijmen et al, Loureiro et al, and Knudsen et al method fails to disclose this process being done iteratively and checking whether the test matrix is nonsingular, and repeating until a nonsingular test matrix has been found.

However, FOLDOC discloses a method of brute force to find something (see page 1).

At the time of the invention it would have been obvious to a person of ordinary skill in the art to use FOLDOC's method of

brute force to find the nonsingular matrix of the modified Rijmen et al, Loureiro et al, and Knudsen et al method.

Motivation to do so would have been to be able to find every solution (see FOLDOC page 1).

6. Claims 6 and 15 are rejected under 35 U.S.C. 103(a) as being unpatentable over the modified Rijmen et al, Loureiro et al, and Williams method as applied to claims 1 and 8 above, and further in view of Isaka et al.

As per claims 6 and 15, the modified Rijmen et al and Loureiro et al method fails to disclose the cipher includes a round function operating on 32-bit blocks and wherein the step of generating a [n,k,d] error-correcting code includes: generating a binary extended Bose-Chaudhuri-Hocquenghem (XRCH) [64,36,12] code;

However, Isaka et al teaches such an XRCH code (see page 3).

At the time of the invention it would have been obvious to a person of ordinary skill in the art to use Isaka et al's XRCH code as the error-correcting code of the modified Rijmen et al, Loureiro et al and Knudsen et al method.

Motivation to do so would have been that these codes achieve unequal error protection (see Isaka et al abstract page 1).

Response to Arguments

7. Applicant's arguments with respect to claims 1, 2, and 6-8 have been considered but are moot in view of the new ground(s) of rejection.

8. Applicant's arguments, filed 03/20/2006, with respect to claims 3 and 16 have been fully considered and are persuasive. The rejection of claim 3 has been withdrawn.

Allowable Subject Matter

9. Claim 16 is allowed.

10. Claims 3-5 and 12-14 are objected to as being dependent upon a rejected base claim, but would be allowable if rewritten in independent form including all of the limitations of the base claim and any intervening claims.

The following is a statement of reasons for the indication of allowable subject matter: with respect to claim 16 which contains the limitations of claims 3 and 12 from which 4-5 and 13-14 respectively depend, the prior art teaches deriving matrix A from matrix C by determining two permutation matrices $P_1, P_2 \in Z_2^{kxk}$ (see Rijmen et al page 5 and Loureiro et al section 4.1). The prior art fails to teach that the determination is

made such that all codewords in an $[2k,k,d]$ error-correcting code, represented by the generator matrix $(I \| P_1 C P_2)$, have a predetermined multi-bit weight. The remaining limitations of claim 16 are taught by the modified Rijmen et al, Loureiro et al, and Knudsen et al method as applied to claims 1 and 8 above.

Conclusion

11. The prior art made of record and not relied upon is considered pertinent to applicant's disclosure. Knudsen et al (Fast and Secure Hashing Based on Codes) teaches shortening error-correcting codes and Youssef et al (On the Design of Linear Transformations for Substitution Permutation Encryption Networks) teaches the use of a generator matrix in an encryption scheme.

Any inquiry concerning this communication or earlier communications from the examiner should be directed to Michael Pyzocha whose telephone number is (571) 272-3875. The examiner can normally be reached on 7:00am - 4:30pm first Fridays of the bi-week off.

If attempts to reach the examiner by telephone are unsuccessful, the examiner's supervisor, Emmanuel Moise can be reached on (571) 272-3865. The fax phone number for the

organization where this application or proceeding is assigned is 703-872-9306.

Information regarding the status of an application may be obtained from the Patent Application Information Retrieval (PAIR) system. Status information for published applications may be obtained from either Private PAIR or Public PAIR. Status information for unpublished applications is available through Private PAIR only. For more information about the PAIR system, see http://pair-direct.uspto.gov. Should you have questions on access to the Private PAIR system, contact the Electronic Business Center (EBC) at 866-217-9197 (toll-free).

MJP

EMMANUEL L. MOISE
SUPERVISORY PATENT EXAMINER